Cara Pendokumentasian Selama Pemblokiran Internet

Mendokumentasikan pelanggaran HAM sama pentingnya selama pemadaman internet. Bahkan jika informasi tidak dapat disebarkan pada saat itu, dokumentasi dapat menjadi cara untuk menjaga suara-suara yang berusaha dibungkam pihak berwenang, serta untuk mengamankan bukti pelanggaran yang dapat digunakan untuk menuntut pertanggungjawaban di kemudian hari.Proses pendokumentasian pelanggaran dan upaya menjaga dokumentasi ini tentu saja menjadi lebih menantang dan berisiko karena represi dan hambatan teknologi selama Pemblokiran Internet. **Bagaimana para aktivis bisa mengambil dan menyimpan video mereka selama "*shutdown*", membagikannya secara offline dan melakukannya dengan lebih aman?**

Menyiapkan Ponsel untuk Dokumentasi Luring

Meskipun terjadi pemadaman internet, para pencatat masih bisa mengambil bukti video penting yang dapat dibagikan secara luring (offline) atau saat mereka bisa kembali daring (online).Berikut adalah beberapa kiat yang kami pelajari dari aktivis dan praktisi lain dalam menyiapkan telepon untuk dokumentasi offline. Perhatikan bahwa beberapa langkah **memerlukan akses internet**, jadi harus dilakukan sebelum *shutdown* terjadi atau selama periode pemulihan. Selain itu, jangan menunggu sampai berada pada situasi penuh tekanan untuk melakukan langkah-langkah ini; lakukan sekarang dan luangkan waktu **untuk berlatih menggunakan telepon ini** sebelum harus digunakan selama krisis.

Pemadaman internet sering bertepatan dengan kontrol terhadap informasi yang meningkat serta pembatasan kebebasan berekspresi dan berkumpul. Jika kamu seorang pencatat melakukan tindakan pencegahan ekstra untuk melindungi diri dan informasi kamu selama periode ini. Jika ada risiko bahwa pihak berwenang akan menyita telepon atau memaksa untuk membuka kunci dan menunjukkan kontennya (selama shutdown atau bukan), pertimbangkan untuk menggunakan telepon untuk dokumentasi yang berbeda dengan telepon pribadi. Hal ini dapat membantu meminimalkan informasi apa yang dapat dikompromikan (mis. kontak, pesan, akun, dll). Jika tidak bisa menggunakan perangkat lain, panduan ini tetap dapat diikuti untuk mengurangi jumlah data sensitif dan meningkatkan keamanan pada telepon utama.

Jika menggunakan telepon lama, bersihkan dan hapus seluruh

Untuk membersihkan telepon, lakukan Factory Reset atau kembalikan pada pengaturan awal

Catatan: Penelitian menunjukkan bahwa melakukan Factory Reset tidak serta merta menghapus semua data. Faktanya, satu-satunya cara yang terbukti aman 100% untuk menghapus data adalah dengan menghancurkan ponsel, tetapi metode itu bukan pilihan jika kamu ingin menggunakan kembali ponsel tersebut! Pada artikel ini, seorang insinyur Android menyarankan untuk memastikan konten pada perangkat kamu dienkripsi sebelum Factory Reset. Enkripsi biasanya merupakan settingan awal pada sebagian besar ponsel saat ini, tetapi jika tidak, buka Pengaturan > Keamanan > Enkripsi Telepon (Settings > Security > Encrypt Phone) sebelum mengatur ulang. Dengan cara ini, ketika dilakukan Factory Reset, kunci enkripsi akan hilang, dan semua data yang tidak terhapus tidak akan bisa dibaca.

Praktik keamanan dasar ponsel

Ada sejumlah praktik keamanan umum ponsel yang masih relevan di segala situasi, baik bagi mereka yang sedang mendokumentasikan selama internet shutdown atau tidak. Berikut ini sejumlah sumber yang berguna bagi organisasi lain. Sementara tidak ada yang menjamin 100% keamanan, sejumlah tips kunci meliputi:

- Pastikan ponsel terenkripsi. Ponsel lebih baru memiliki enkripsi secara stkamur. Kalau tidak yakin dengan ponsel yang digunakan, cek pengaturan keamanan di ponsel.
- Jalankan pemutakhiran Sistem Operasi secara rutin, karena kerap ada perbaikan celah keamanan.
- Perbaharui secara rutin aplikasi yang penting (seperti aplikasi Pesan Instan).
- Tetapkan kode sandi ponsel yang kuat yang memiliki setidaknya 6 digit dan tidak bergantung pada sidik jari / sentuhan atau ID wajah.
- Atur penguncian layar dan penguncian waktu.
- Matikan layanan lokasi jika kamu tidak membutuhkannya (termasuk layanan lokasi darurat, akurasi lokasi, riwayat lokasi, dan fitur berbagi lokasi, dan opsi pemindaian WiFi dan Bluetooth). Periksa juga izin lokasi untuk masing-masing aplikasi.
- Matikan Bluetooth dan WiFi saat tidak dibutuhkan, untuk menghindari pelacakan gawai.
- Matikan ponsel saat tidak digunakan.

Instal aplikasi dokumentasi yang berguna

Untuk dokumentasi foto atau video, gunakan aplikasi kamera bawaan pada ponsel atau dapat menggunakan aplikasi dokumentasi yang lebih khusus, seperti ProofMode atau yang lainnya, yang memungkinkan penangkapan metadata yang lebih kuat dan ekspor, identifikasi dan otentikasi, enkripsi, galeri aman, atau fitur lainnya.

Aplikasi yang berguna untuk mendokumentasikan suatu shutdown adalah OONI Probe, aplikasi open-source yang menjalankan tes dari ponsel kamu untuk mengukur apakah situs atau platform sedang diblokir. Ini dapat menunjukkan bagaimana, kapan, di mana, dan oleh siapa situs diblokir. Pastikan untuk memahami risiko potensial sebelum menggunakan aplikasi ini.

Tidak yakin aplikasi dokumentasi mana untuk digunakan? Kami sediakan beberapa pertanyaan panduan dalam tutorial "Haruskah Saya Menggunakan Aplikasi Dokumentasi ini?".

Menginstall beberapa aplikasi sehari-hari

Hanya memiliki sedikit data dan aplikasi khusus di ponsel bisa memunculkan kecurigaan. Agar perangkat terlihat seperti ponsel sehari-hari, pasanglah beberapa aplikasi yang umumnya digunakan di lokasi di mana kamu melakukan dokumentasi (tetapi mereka diunduh dari sumber-sumber tepercaya), dan mengambil beberapa foto tidak berbahaya dari galeri kamu.

Untuk aplikasi media sosial, kamu mungkin bisa membuat dan masuk akun-akun alternatif, meskipun harus diingat bahwa akun palsu melanggar Ketentuan Penggunaan sebagian besar platform, dan persyaratan verifikasi identitas beberapa aplikasi mungkin susah dipalsukan. Selain itu, kamu juga memerlukan waktu lebih lama untuk membuat konten dan menambahkan teman, yang bisa melelahkan.

Menginstall aplikasi ketika tidak ada internet

Mengunduh dan menginstal aplikasi tanpa akses internet jelas merupakan tantangan. kamu perlu mengunduh aplikasi terlebih dahulu jika kamu ingin mengantisipasi adanya pemadaman internet.

Salah satu strategi yang dapat membantu kamu dan orang lain di kemudian hari adalah mengunduh dan menyimpan file Paket Android (.apk) untuk aplikasi (**diunduh dari sumber terpercaya**, mis. Langsung dari pengembang) di penyimpanan ponsel atau di drive. Memiliki APK ini secara offline memungkinkan kamu atau orang lain untuk berbagi aplikasi ketika tidak ada internet.

Meskipun kami belum berkesempatan mencobanya, aplikasi F-Droid menyediakan antarmuka untuk menukar APK ini secara offline. Inilah tutorial mereka.

Cobalah untuk memiliki perangkat khusus untuk melakukan dokumentasi. Jangan menggunakannya untuk email, panggilan telepon, atau pesan dengan kontak pribadi atau aktivis yang dapat berisiko, dan jangan sambungkan perangkat ini ke akun riil dan/atau akun utama kamu.

Gunakan fitur-fitur untuk mengaburkan konten

- Jika ponsel kamu diutak-atik, mungkin akan membantu jika pada ponsel, niat kamu kurang jelas terlihat atau konten kamu lebih sulit ditemukan. Untuk mengantisipasi situasi di mana ponsel kamu hanya akan diperiksa (orang lain) secara dangkal dan cepat, kamu dapat menggunakan taktik sederhana seperti:

- Mengubah nama dan ikon pintasan aplikasi dengan menggunakan aplikasi Launcher (mis. Nova Launcher, tetapi ada banyak ikon dan nama yang sama) sehingga kurang jelas apa itu aplikasi tertentu.

- Menggunakan fitur privasi bawaan seperti Mode Pribadi (Samsung) atau Content Lock (LG), jika ponsel kamu mendukungnya.

- Menempatkan file kosong bernama ".nomedia" di dalam folder apa saja yang ada, untuk mencegah media di folder muncul di galeri kamu. Catatan: Jika media masih muncul, kamu mungkin perlu menghapus cache Galeri kamu. Ini mungkin tidak sama hasilnya di semua perangkat.

- Membuat folder tersembunyi (folder yang dimulai dengan ".") dengan menggunakan aplikasi manajer file. kamu dapat memindahkan file ke folder tersembunyi tersebut secara manual, atau jika bisa juga menggunakan aplikasi kamera seperti Open Camera. kamu dapat menentukan di mana media yang kamu rekam disimpan. Pastikan untuk mematikan opsi "tampilkan file tersembunyi" di Pengaturan kamu sehingga file yang tersembunyi tidak terlihat.

- Beberapa aplikasi dokumentasi khusus, seperti Tella, menyimpan dokumentasi di galeri terenkripsi terpisah yang isinya hanya dapat diakses di dalam aplikasi, mungkin membuatnya kurang dapat dilihat jelas bagi seseorang yang mengutak-atik mencari-cari di ponsel kamu. Dokumentasi di galeri yang aman ini memerlukan kode sandi aplikasi yang terpisah, sehingga tetap dienkripsi bahkan ketika ponsel kamu tidak terkunci.

Catatan penting tentang mengaburkan konten kamu

Penting untuk dicatat bahwa teknik-teknik di atas mungkin cukup untuk membuang seseorang yang dengan cepat menggeser-geser tampilan ponsel kamu, tetapi tidak akan secara efektif menyembunyikan konten kamu dari seseorang yang benar-benar melihat.

Ingat juga bahwa beberapa negara mungkin memiliki undang-undang yang membatasi atau mengkriminalkan penggunaan aplikasi keamanan yang mengenkripsi atau menghapus data kamu. Menggunakan aplikasi tersebut untuk mencegah pihak berwenang mengakses data kamu dapat dilihat sebagai menghancurkan bukti atau menghambat penyelidikan, dan dapat dihukum sebagai kejahatan. Peta ini (komprehensif, tetapi dibuat pada tahun 2017) memberikan awalan yang baik jika kamu memiliki pertanyaan tentang undang-undang di negara kamu.

Persiapan Berbagi Luring/Offline

Ketika berada dalam situasi offline/luring, kamu mungkin ingin tetap menghapus beberapa dokumentasi, baik atas dasar keamanan, memperluas penyimpanan, atau membagikannya dengan orang lain. Menghapus dokumentasi secara rutin di ponsel kamu, akan membantu mengurangi informasi jika dicuri atau dibuka kunci pengamannya.

Walaupun kamu tidak terhubung ke internet, kamu tetap dapat mengakses wifi atau bluetooth lokal yang ada di dalam ponsel, seperti melalui ponsel lain atau perangkat wifi USB. Ponsel kamu seharusnya sudah memiliki sebuah aplikasi untuk terhubung dengan kedua fitur diatas. Jika mendukung, kamu dapat memasang perangkat USB On-The-Go (OTG) guna memindahkan dokumentasi ke perangkat lain.

Metode tersebut dapat didiskusikan secara lebih rinci di tutorial “Cara berbagi data dan berkomunikasi ketika Internet Shutdown” dan video “As Evidence: Tech Tools — Transferring Files”.

Berlatihlah sebelum kamu berada dalam situasi krisis

Atur telepon sekarang jika dan sementara kamu sedang memiliki akses internet. Mulai berlatih menggunakan aplikasi dalam situasi sehari-hari (di mana tidak ada masalah keamanan) agar terbiasa dan nyaman menggunakannya. Jadikan keamanan dasar telepon yang baik sebagai praktik default kamu. Dengan cara ini, metode yang digunakan kemudian akan menjadi hal yang wajar ketika kamu berada dalam situasi krisis saat banyak hal yang perlu dikhawatirkan.

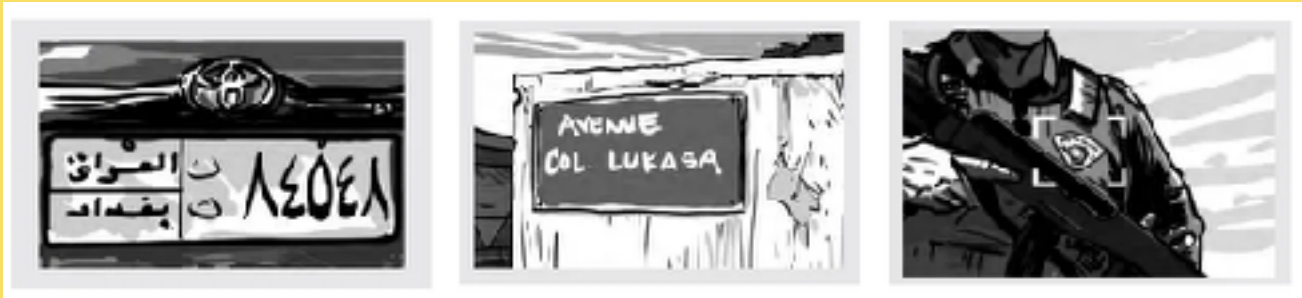
Haruskah Saya Menggunakan Aplikasi Dokumentasi Ini?

Ada banyak aplikasi yang dapat digunakan oleh para pembuat dokumentasi untuk mengambil video, mulai dari aplikasi kamera bawaan ponsel kamu, hingga aplikasi dokumentasi yang lebih khusus seperti ProofMode atau Tella. Beberapa aplikasi memiliki fitur yang mengkamulkan akses internet, jadi perlu diingat bahwa fitur tersebut mungkin tidak tersedia jika terjadi pemadaman internet.

Kami tidak dapat memberi tahu kamu aplikasi spesifik mana yang paling tepat untuk kamu, karena tergantung dari situasi, kebutuhan, dan risiko (lihat posting blog ini untuk informasi lebih lanjut tentang cara menilai risiko dan ancaman kamu). Dengan penilaian risiko, pertanyaan panduan di bawah ini dapat membantu untuk mengevaluasi aplikasi dokumentasi video mana yang paling cocok untuk kamu.

Mempertahankan Media yang dapat diverifikasi selama Internet Shutdown

- Pembela HAM, penyidik, peneliti, dan jurnalis biasanya bergantung pada dokumentasi awal dari saksi untuk melakukan pemantauan, pelaporan, dan menganalisis pelanggaran HAM. Guna memastikan mereka tetap menggunakan informasi yang tepat, pengguna-pengguna ini dapat melakukan otentifikasi dan verifikasi dokumentasi yang mereka dapatkan--dimana proses ini memakan waktu yang cukup lama.
- Sebagai pendokumentasi, terdapat beberapa langkah sederhana yang dapat kamu lakukan dalam melakukan verifikasi dan memperkuat informasi, sehingga dapat digunakan secara efektif dan sesuai. Berikut beberapa langkah ekstra yang mungkin dapat berguna selama Internet Shutdown, yang mempertimbangkan:
- Jika kamu tidak dapat mengunggahnya langsung, fitur tanggal dan lokasi dari publikasi yang disediakan oleh media sosial tidak cukup bermanfaat untuk menunjukan bahwa video tersebut direkam pada tanggal atau lokasi tertentu
- Jika rekan lainnya tidak dapat mengunggah juga, akan sangat sedikit dokumentasi yang tersedia secara keseluruhan yang dapat digunakan untuk memperkuat video kamu
- Jika kamu membutuhkan untuk menggeser perekam kamu ke banyak orang secara offline untuk sampai ke lokasi tujuan, akan sangat sulit bagi yang lainnya untuk melacak sumber video tersebut
- Jika kamu ingin menghapus video asli dari ponsel kamu karena pertimbangan keamanan atau kapasitas memori yang terbatas, atau jika kamu ingin menyingkirkan ponsel tersebut, akan sangat sulit untuk mengkonfirmasi keaslian dari video tersebut.
- Jika kamu lupa rincian dari video tertentu dan aplikasi yang digunakan tidak mencatat rincian tersebut, rekan lain mungkin akan sulit mengidentifikasinya di masa depan.

Saran di bawah ini dapat membantu kamu menjaga kualitas video kamu selama Internet Shutdown Film atau mengidentifikasi rincian di dalam video

Sertakan rincian di dalam video kamu sehingga dapat memudahkan bagi penyidik atau jurnalis dalam mengidentifikasi waktu dan tempat, seperti pertkamu unik, garis langit, tkamu jalan, etalase toko, plat kendaraan, bendera, jam, halaman depan koran, dan lainnya. kamu juga dapat menarasikan informasi dasar seperti nama kamu dan informasi kontak (jika aman), waktu, tanggal, dan lokasi atau koordinat GPS. Semakin rinci informasi tersebut, akan semakin mudah bagi orang lain dalam melakukan pencarian dan memverifikasi video tersebut di kemudian hari.

Cari tahu saran lain di Basic Practices for Capturing, Storing, and Sharing.

Menambahkan deskripsi/metadata

Ambil keuntungan dari aplikasi yang memiliki fitur dokumentasi yang spesifik menggunakan metadata atau informasi teknis dari dalam ponsel, dan izinkan agar dapat secara manual menambahkan informasi deskriptif lain. Perlu diingat bahwa selama Internet Shutdown, dibutuhkan sebuah aplikasi yang tidak bergantung pada akses internal untuk merekam atau menyimpan metadata.

Bahkan jika kamu tidak menggunakan sebuah aplikasi yang memiliki fitur dokumentasi spesifik, kamu tetap dapat membuat informasi tambahkan ke dalam lembar catatan, peta, atau foto dalam ponsel kamu. kamu dapat membuat video kamu dengan informasi tambahan tersebut dengan menggunakan aplikasi file manager favorit kamu.

Informasi tambahan kunci meliputi waktu, tanggal, lokasi, dan juga sumber perekaman (nama kamu dan kontak informasi, jika aman). Pindahkan kedalam metadata dan sertakan itu kedalam sebuah video ketika membagikannya.

Simpanlah Cadangan

Cadangkan media dari ponsel kamu secara rutin, idealnya dua kali di dalam dua perangkat penyimpanan yang berbeda. kamu dapat menghubungkannya dengan OTG atau perangkat wireless ke ponsel, bahkan tanpa komputer.

Menyimpan cadangan dapat meminimalisir salinan video hilang jika ponsel kamu hilang atau hancur, atau kamu butuh untuk menghapus video dari ponsel.

Memiliki salinan yang aman dari video asli juga dapat membuat kerja penyidik atau jurnalis menjadi lebih mudah.

Mencadangkan Media Ponsel Tanpa Internet atau Komputer

Cadangan merupakan kunci dalam memastikan data dan dokumentasi kamu tidak terhapus, rusak, atau hilang secara tiba-tiba apabila perangkat kamu hilang.

Selama Internet Shutdown atau penurunan kecepatan internet, kamu mungkin tidak dapat secara rutin mengoperasikan cadangan *cloud* atau mengirimkan dokumentasi kamu ke lokasi penyimpanan yang aman.

Memindahkan dari desktop atau komputer merupakan cara lain dalam melakukan pencadangan, namun sejak banyak orang tidak memiliki akses kesana, berikut beberapa pilihan dan saran untuk mencadangkan media dari ponsel kamu selama internet shutdown tanpa komputer.

Gunakan OTG atau Drive Nirkabel

OTG atau perangkat *on-the-go*, merupakan tipe USB yang cocok dengan banyak (tidak semua) Android. kamu dapat memasang perangkat kabel OTG secara langsung ke ponsel kamu, atau menggunakan adapter *OTG-to-USB* untuk menghubungkan ponsel kamu ke perangkat keras USB yang reguler. Dengan OTG, ponsel kamu menyediakan daya ke perangkat.

Merek populer dari OTG termasuk SanDisk, Kingston, dan Samsung, meskipun sebenarnya ada banuak lainnya. Biasanya seharga 8-25 USD tergantung dari kapasitas penyimpanan.

Perangkat wireless/perangkat keras serupa dengan perangkat keras pada umumnya, kecuali tidak memerlukan kabel. Hal ini menghubungkan perangkat yang tidak secara normal menghubungkan ke perangkat keras, seperti ponsel kamu.

Keunggulan dari perangkat wireless dari perangkat OTG adalah kamu dapat menghubungkan banyak pengguna ke satu perangkat dalam waktu bersamaan. Hal ini dapat bermanfaat, misalnya, ketika dalam situasi protes ketika kamu sedang membuat film dalam sebuah tim--semua rekaman dari tiap orang dapat dicadangkan ke sebuah perangkat keras yang tiap anggota tim lain dapat gunakan.

Perhatikan apabila mereka tidak membutuhkan daya dari sebuah perangkat, perangkat wireless bergantung pada daya baterai dan membutuhkan pengisian.

SanDisk mungkin sebuah brand yang paling populer dari perangkat keras, walaupun ada yang lainnya. Perangkat wireless secara umum lebih mahal dari perangkat OTG, dan berkisar antara 25-100 USD tergantung pada kapasitas penyimpanan. Perangkat keras eksternal mulai berkisar dari 150 USD tergantung pada kapasitas penyimpanan.

Alternatif: Gunakan ponsel lama yang tidak terpakai

Jika tidak memiliki OTG atau perangkat wireless, tetapi memiliki ponsel lama yang tidak digunakan tetapi masih berfungsi, kamu juga bisa menggunakannya sebagai cadangan. Selama kedua ponsel berada dalam jangkauan fisik, kamu bisa menyambungkan dan menyalin media dari satu perangkat ke perangkat lainnya melalui Bluetooth, WiFi Direct, atau Near Field Communication (NFC)/Android Beam. Bluetooth dan WiFi Direct merupakan teknologi nirkabel yang dapat menyambungkan kedua perangkat tanpa menggunakan router atau access point di antara keduanya. WiFi Direct menyediakan cakupan yang lebih luas dan data transfer yang lebih cepat daripada Bluetooth, tetapi menghabiskan lebih banyak energi. Sedangkan NFC memiliki jangkauan yang jauh lebih pendek (~4 cm) dan kecepatan transfer yang lebih lambat, tetapi terhubung lebih cepat dan menggunakan daya yang lebih hemat, sehingga berguna untuk mengalihkan sesuatu yang kecil dengan cepat jika memiliki kedua perangkat di tangan.

Ponsel kamu barangkali telah dilengkapi dengan fitur Bluetooth, WiFi Direct, atau NFC bawaan yang memungkinkan dapat memilih perangkat mana yang bisa dibagikan. Jika pada kedua ponsel terpasang Files By Google, kamu juga bisa membagikan file secara offline menggunakan aplikasi tersebut.

Penting: kekurangan dari kemudahan koneksi yang disediakan oleh layanan tersebut adalah ketidakamanan. Bluetooth dan pemindai wifi dapat digunakan untuk melacak lokasi atau menyelidiki perangkat kamu demi mendapatkan informasi. Penyusup dapat mencoba untuk terhubung dengan perangkat kamu, mengirimi file yang tidak diinginkan, atau bahkan menguasai perangkat jika rentan. **Agar lebih aman, matikan layanan ini ketika tidak digunakan dan hanya dinyalakan saat berada di tempat yang aman, batasi izin aplikasi hanya untuk apa / siapa yang dibutuhkan, serta praktikkan keamanan ponsel yang baik; seperti melakukan pembaruan dan menggunakan kata sandi yang kuat.**

Sertakan deskripsi/metadata yang terpisah

Saat menyalin media ke perangkat OTG, perangkat nirkabel, atau ponsel lama, ada baiknya menyertakan informasi deskriptif atau metadata yang mungkin terpisah dari media. Banyak aplikasi dokumentasi menghasilkan dokumen teks CSV atau JSON yang menyertakan metadata yang ditarik dari perangkat (mis. Geolokasi, waktu, tanggal) dan deskripsi apapun yang dimasukkan secara manual oleh pengguna. Pastikan untuk mengekspor dan memasukkan dokumen metadata ini ke dalam cadangan juga.

Lindungi perangkat dengan kata sandi

Banyak drive nirkabel dapat dilindungi oleh kata sandi dengan aplikasi seluler yang disertakan bersama drive tersebut. Perhatikan bahwa perlindungan kata sandi tidak sama dengan enkripsi (lihat di bawah). Sebagian besar drive nirkabel atau OTG tidak bisa mengaktifkan *full-disk encryption* (FDE) jika hanya menggunakan ponsel, meskipun drive tersebut mungkin dienkripsi dengan penuh jika menggunakan komputer.

Pertimbangkan untuk mengenkripsi file

Jika ingin menyimpan file dengan lebih aman, kamu mungkin perlu mempertimbangkan untuk mengenkripsi file cadangan. Meskipun kamu mungkin tidak dapat mengenkripsi sebagian besar drive nirkabel atau OTG dengan ponsel, tetapi kamu dapat mengenkripsi file itu sebelum dipindahkan ke drive. Beberapa aplikasi dapat digunakan untuk mengenkripsi file di Android termasuk ZArchiver, dan RAR. Ketahuilah bahwa kata sandi enkripsi harus diingat, karena tidak ada cara untuk memulihkan file yang terenkripsi jika kamu kehilangan kata sandi.

Perlu diingat bahwa beberapa negara mungkin memiliki undang-undang yang membatasi atau mengkriminalisasi penggunaan enkripsi. Menggunakannya untuk mencegah pihak berwenang mengakses data kamu dapat dianggap menghancurkan bukti atau menghambat penyelidikan, dan dapat dihukum sebagai kejahatan. Peta 2017 ini mungkin sudah usang tetapi menyediakan informasi awal yang baik jika memiliki pertanyaan tentang undang-undang di negara kamu.

Buat 2 cadangan di lokasi yang berbeda

Satu cadangan tidak selalu dapat dikamulkan. Misalnya, kamu mungkin kehilangan perangkat cadangan, merusaknya, atau mungkin gagal secara acak. Pakar TI biasanya menyarankan orang untuk memiliki 2 cadangan (mis. total 3 salinan), pada perangkat berbeda yang disimpan di lokasi terpisah. Ini membantu mengurangi berbagai risiko terhadap satu salinan tertentu.

Berbagi File dan Komunikasi Selama Internet Shutdown

Internet shutdown dirancang untuk memblokir orang dari berbagi informasi dan berkomunikasi (dan juga mendorong orang ke bentuk komunikasi yang kurang aman seperti ponsel dan SMS, yang lebih mudah bagi pihak berwenang untuk menyadap dan memantau). Tidak selalu ada solusi yang baik selama total internet shutdown. Selama periode ketat penutupan di Kashmir, misalnya, menggunakan catatan tulisan tangan dan kurir untuk mengirim pesan ke orang yang mereka cintai.

Kami tidak memiliki cara ampuh untuk menghindari semua pencekikan internet, tetapi melalui percakapan dengan aktivis dan rekan-rekan, kami telah mempelajari beberapa metode dan pendekatan untuk berbagi offline dan komunikasi yang mungkin bekerja untuk kamu, tergantung pada keadaan. Perhatikan bahwa beberapa opsi ini memerlukan pengaturan internet pada awalnya (mis. Untuk mengunduh aplikasi, dll).

Berbagi dokumen secara langsung lewat Bluetooth, Wifi Direct, atau NFC

Kamu tidak perlu memiliki koneksi internet untuk menghubungkan ponselmu dengan perangkat terdekat lainnya melalui Bluetooth, Wifi Direct, atau Near Field Communication (NFC) (kadang-kadang disebut Android Beam pada perangkat yang lebih lama). Bluetooth dan Wifi Direct adalah teknologi nirkabel yang dapat "memasangkan" dua perangkat tanpa router atau titik akses di antaranya. WiFi Direct menyediakan jangkauan yang lebih luas dan transfer data yang lebih cepat daripada Bluetooth, tetapi menggunakan daya yang jauh lebih besar. Sementara itu, NFC memiliki jangkauan yang jauh lebih pendek (~ 4cm) dan kecepatan transfer yang lebih lambat daripada Bluetooth atau WiFi Direct, tetapi menghubungkan lebih cepat dan menggunakan daya lebih sedikit, sehingga dapat berguna untuk transfer kecil ketika kedua perangkat berada di tangan kamu.

Kamu mungkin memiliki fitur Bluetooth, WiFi Direct, dan NFC di dalam ponselmu yang muncul dalam opsi berbagi kamu. Selain itu, aplikasi dengan fitur berbagi file, seperti Files By Google, juga mengintegrasikan teknologi ini.

Catatan Penting: kerugian dari kemudahan koneksi yang disediakan oleh layanan ini adalah bahwa mereka tidak aman. Bluetooth dan wifi beacon / scanner dapat digunakan untuk melacak lokasimu atau menyelidiki perangkatmu untuk mendapatkan informasi. Penyusup dapat mencoba memasangkan dengan perangkatmu, mengirimimu file yang tidak diinginkan, atau bahkan menguasai perangkatmu jika rentan. Agar lebih aman, matikan layanan ini ketika kamu tidak menggunakannya dan hanya nyalakan saat kamu berada di tempat yang aman, batasi izin aplikasi hanya untuk apa / siapa yang kamu butuhkan, dan praktikkan keamanan telepon yang baik seperti menjalankan pembaruan dan memiliki kekuatan kode sandi.

Berbagi dokumen lewat hard drive nirkabel atau via Wireless Local Area Network (WLAN)

Hard drive nirkabel atau flash drive dapat digunakan untuk berbagi file di antara tim, atau beberapa orang sekaligus. Drive wifi biasanya datang dengan instruksi dan / atau aplikasi untuk menghubungkan ponselmu ke drive, dan relatif mudah digunakan. Ingatlah untuk mengatur kata sandi di drive untuk keamanan.

Jika kamu tidak memiliki drive nirkabel, kamu juga dapat berbagi file di drive USB biasa dengan menghubungkannya ke router nirkabel. Router perjalanan dengan port USB, misalnya, relatif murah dan sangat portabel. Pengguna dapat terhubung ke drive USB melalui jaringan lokal (tidak perlu internet). Untuk mengakses file pada drive USB yang terhubung pada ponselmu, kamu harus menggunakan aplikasi manajer file yang dapat terhubung ke penyimpanan jaringan, seperti Solid Explorer. Alamat IP router kamu biasanya dapat ditemukan di pengaturan wifi canggih ponselmu.

Sementara itu, opsi lain adalah PirateBox, proyek do-it-yourself yang menyediakan perangkat lunak berlisensi gratis. Pengguna dapat berbagi file seperti di atas, tetapi Piratebox memungkinkan mereka melakukannya secara anonim, dan juga menyertakan fitur obrolan dan pesan. Menyiapkan Piratebox membutuhkan pengunduhan, penginstalan, dan pengaturan beberapa perangkat lunak. Instruksi ada di situs web PirateBox.

*Project Piratebox saat ini sudah tidak aktif dan jarang diperbarui. Anda dapat mencek projek alternatif TheLibraryboxProject.

Komunikasi lewat percakapan Peer-to-Peer (P2P)

Dua aplikasi peer-to-peer perpesanan baru yang kami ketahui melalui jaringan aktivis adalah Briar dan Bridgefy. Kami belum mencobanya, tetapi kami tahu orang lain yang mengujinya.

Briar adalah aplikasi pesan terenkripsi open-source terpercaya, yang tidak bergantung pada server pusat, melainkan menyinkronkan pesan di antara perangkat pengguna (sehingga konten tinggal di perangkat masing-masing pengguna). Itu dapat menyinkronkan bahkan ketika tidak ada internet menggunakan Bluetooth atau WiFi (ketika ada internet, aplikasi menyinkronkan perangkat melalui jaringan Tor). Briar juga menampilkan grup pribadi, forum publik, dan blog. Saat menggunakan offline, jangkauanmu dibatasi oleh rentang Bluetooth atau WiFi (maksimum ~ 100 meter).

Sementara itu, Bridgefy adalah aplikasi pesan terenkripsi terpercaya (kecuali ketika menggunakan fitur "siaran") yang menggunakan Bluetooth untuk mengirim pesan. Tidak seperti Briar, pesan dapat menempuh jarak yang lebih jauh dengan melompat di sepanjang jaringan mesh dari pengguna Bridgefy lainnya (hanya penerima yang dituju dapat membaca pesan). Bridgefy tidak memiliki grup pribadi Briar, forum, dan fitur blog, tetapi memiliki mode Broadcast agar kamu dapat mengirim pesan ke hingga 7 pengguna Bridgefy dalam jangkauan, yang tidak perlu menjadi kontakmu (pesan Broadcast karena kebutuhan tidak terenkripsi).

Komunikasi lewat SMS terenkripsi

Pesan teks SMS dikirim melalui jaringan seluler dan tidak bergantung pada internet, jadi mungkin masih berfungsi selama internet shutdown. Namun, SMS dianggap sangat tidak aman. Tidak seperti aplikasi yang bergantung pada internet seperti WhatsApp atau Signal, SMS tidak dienkripsi end to end. Ini berarti bahwa pesan teks (dan metadata mereka) dapat dibaca oleh pemerintah dan operator seluler, atau dicegat oleh peretas. SMS juga dapat "dipalsukan," yang berarti bahwa pengirim dapat memanipulasi informasi alamat mereka untuk menyamar sebagai pengguna lain.

Jika kamu perlu menggunakan SMS, Silence adalah aplikasi yang mengenkripsi pesan SMS secara end to end. Ini adalah open source program dan menggunakan protokol enkripsi Signal. Meskipun kami belum mencobanya sendiri, kami telah mendengar bahwa orang lain telah menggunakannya. Baik pengirim dan penerima harus menginstal dan bertukar kunci satu sama lain. Karena pesan SMS harus melalui server telekomunikasimu, bahkan dengan Silence kenyataan bahwa kamu mengirim pesan terenkripsi dan metadata tentang pesanmu akan dapat diakses oleh perusahaan telekomunikasi.

Shutdown sebagian: Memotong pemblokiran situsweb

"Internet shutdown" seringkali tidak berarti pemadaman internet total, melainkan memblokir akses ke situs web atau platform media sosial tertentu. Pemerintah, melalui penyedia layanan internet (ISP), dapat memblokir situs berdasarkan alamat IP, konten, atau melalui pencarian DNS. Tidak yakin apakah suatu situs sedang diblokir? Organisasi seperti Open Open Observatory of Network Interference (OONI) dan Netblocks memantau dan mengukur gangguan internet dan sensor di seluruh dunia. Untungnya, selama kamu memiliki akses internet, ada beberapa cara untuk mencoba menyiasati sebagian blok. Seperti halnya enkripsi, perlu diingat bahwa menghindari situs yang diblokir dapat dikriminalisasi di negaramu.

VPN

Salah satu cara untuk memotong pemblokiran berbasis IP dan berbasis konten adalah dengan menggunakan VPN, seperti ProtonVPN atau TunnelBear. Ketika kamu terhubung melalui VPN, lalu lintas internet kamu dienkripsi dan dialihkan melalui server VPN di lokasi lain, seperti di negara lain, sehingga menyembunyikan tujuan sebenarnya dan konten lalu lintas kamu ke ISP.

Ingatlah bahwa beberapa pemerintah melarang penggunaan VPN atau mungkin mencoba mendeteksi dan memblokir koneksi VPN. Penting juga untuk menggunakan penyedia VPN yang dapat dipercaya, dan lebih disukai yang tidak menyimpan data atau log, karena penyedia akan dapat melihat aktivitas internetmu. Berhati-hatilah dengan negara mana penyedia VPN itu berada, dan proses hukum apa yang harus mereka patuhi berdasarkan yurisdiksinya. Juga pertimbangkan bahwa VPN yang disetujui pemerintah sebenarnya dapat mengaktifkan pengawasan dan inspeksi datamu.

Server DNS

Server DNS ("sistem nama domain") berfungsi dengan menerjemahkan nama domain atau URL yang diketik pengguna ke dalam browser ke alamat IP numerik yang digunakan internet untuk mengidentifikasi halaman web. ISP dapat memodifikasi server DNS yang dikontrolnya untuk memblokir pertanyaan tertentu, atau untuk mengembalikan halaman yang salah yang mengatakan bahwa situs web itu tidak ada.

Pada tahun 2014, Perdana Menteri Turki Recep Tayyip Erdoğan berusaha memblokir Twitter selama pemilihan umum Turki menggunakan teknik ini. Larangan itu dengan cepat digagalkan oleh aktivis yang berbagi kiat langkah demi langkah tentang cara menggunakan VPN dan mengubah server DNS.

Kamu dapat mengubah server DNS default di jaringan atau pengaturan wifi ponsel kamu. Alih-alih server DNS default, kamu dapat menggunakan server DNS alternatif seperti Google Public DNS atau CloudFlare untuk menyiasati blok berbasis DNS. Cloudflare juga memiliki aplikasi bernama 1.1.1.1 yang memungkinkan pengguna untuk beralih ke server DNS Cloudflare melalui antarmuka aplikasi sederhana.

Ini hanya dua cara untuk menghindari teknik pemblokiran yang paling umum. Lihatlah panduan bermanfaat dari Internet Society, Access Now, Security-in-a-Box, dan EFF untuk informasi lebih lanjut.